プロメテウス：検証可能で高度な分散型金融のためのプロトコル

著者: Masahiro Aoki
ドキュメントID：MT2025-BC-01-002
ORCID ID：0009-0007-9222-4181
所属: Moonlight Technologies 株式会社

文書バージョン	作成日	作成者	概要
Ver 1.0	2025年8月12日	Masahiro Aoki	初版

要旨

プロジェクト「プロメテウス」は、規制され、高性能なグローバル金融システムの基盤インフラとして機能するために設計された、次世代のレイヤー1プロトコルである。本プロジェクトは、第一世代ブロックチェーンに内在するトレードオフ、すなわち絶対的な分散化と実用的なユーティリティとの間の緊張関係に対処するため、「分散化」「セキュリティ」「スケーラビリティ」「検証可能なコンプライアンス」という4つの柱によって定義される新たな設計空間を明示的に最適化する。本稿では、三層からなる共生的なアーキテクチャを詳述する。すなわち、新規性の高いハイブリッド・プルーフ・オブ・ステーク・アンド・レピュテーション（HPoSR）コンセンサスメカニズムによって保護される**アイデンティティ＆ガバナンス層（IGL）**、NarwhalとMysticetiに着想を得た最先端のDAG-BFTモデルに基づいて2秒未満の決定的ファイナリティを達成する**トランザクション＆ファイナリティ層（TFL）**、そして適応型ゼロ知識証明（ZKP）と閾値暗号を用いてオンチェーンの機密性と規制要件を両立させる**プライバシー＆監査可能性層（PAL）**である。プロトコルは、デフレ的な手数料焼却メカニズムを特徴とするPROトークンによって駆動され、多様なステークホルダーの利益を均衡させるために設計された、強靭な二院制フレームワークによって統治される。これらのイノベーションを統合することにより、プロメテウスは、分散型金融と主流の機関投資家による採用との間のギャップを埋めることが可能な、堅牢でスケーラブル、かつコンプライアンスに準拠したプラットフォームを提供することを目指す。

1. 序論：プロメテウスの責務 - 思想的純粋性から実用的ユーティリティへ

1.1. 第一世代プロトコルの遺産とその根源的トレードオフ

2009年にビットコインが登場して以来、トラストレスな価値移転という概念は、金融とテクノロジーの世界に革命的な影響を与えてきた。しかし、その後の進化の過程で、ビットコインのような第一世代プロトコルの設計に内在する根源的なトレードオフが明らかになった。これらのトレードオフは「欠陥」ではなく、特定の思想的目標を達成するために意図的に受け入れられた設計上の選択である。

- **スケーラビリティ:** 1MBのブロックサイズと約10分間のブロック生成間隔という制約により、ビットコインのトランザクション処理能力は毎秒約7件（TPS）に制限される。これは、数万TPSを処理するVisaのような既存の決済システムとは比較にならず、ネットワークの利用が増加すると、深刻な混雑と手数料の高騰を引き起こす。

- **エネルギー消費:** プルーフ・オブ・ワーク（PoW）コンセンサスメカニズムは、膨大な計算能力を投入することで堅牢なセキュリティを確保するが、その代償として年間約178TWhという莫大な電力を消費する。これはポーランド一国の年間消費量に匹敵し、環境持続可能性の観点から大きな課題となっている。
- **経済的実用性:** 国家による価値の裏付けを持たないため、その価格は主に市場の期待と投機によって形成される。結果として、年率換算ボラティリティは50%を超えることもあり、日常的な決済手段としての安定性に欠ける。さらに、富の集中も著しく、ジニ係数は0.94に達し、上位0.01%のアドレスが流通供給量の42%以上を保有している。
- **規制との摩擦:** かつての追跡の困難さから、違法行為に利用されるケースがあり、これが世界的な規制強化の動きを加速させる一因となった。
- **価値の源泉:** ビットコインの価値は、物理的な裏付け資産を持たず、純粋に需要と供給、そして参加者の信頼に基づいている。この「内在的価値の欠如」は、長期的な価値保存手段としての安定性に対する根源的な問いを投げかけている。

これらのトレードオフはすべて、ビットコインが「絶対的な検閲耐性」という至上命題を追求した結果である。プロジェクト「プロメテウス」は、この思想的達成を尊重しつつも、その優先順位を根本的に転換する必要性を認識している。

1.2. 設計上の至上命題の再定義：主流採用のための金融インフラ

プロメテウスの核心的なビジョンは、最適化の焦点を「絶対的な分散化」から「実用的なユーティリティ」へと移行させることにある。その目標は、ビットコインを改良することではなく、主流の金融システムに統合され、日常的に利用されることを前提とした、根本的に異なる種類のインフラをゼロから構築することである。

このビジョンを実現するためには、当初の設計思想をさらに深化させる必要がある。当初の設計は、第一世代プロトコルの限界を正しく認識していたが、その解決策は、複雑な技術の過度な単純化に起因する脆弱性を内包していた。例えば、評判への依存はシビル攻撃のリスクを看過し、曖昧なファイナリティは金融システムとしての信頼性を損ない、ZKPのパフォーマンスコストはユーザーエクスペリエンスを非現実的なものにしていた。

したがって、プロメテウスの設計哲学は、「評判に基づく信頼の仮定」から、「検証可能な完全性の強制」へと昇華されなければならない。この新しい哲学では、信頼は出発点となる仮定ではなく、巧みに設計された暗号学的証明（検証可能クレデンシャルとゼロ知識証明）と経済的インセンティブ（ステーキングと報酬）のシステムから「創発」される特性となる。このアプローチこそが、プロトコル全体のアーキテクチャを貫く指導原理である。

2. 設計哲学：現代金融プロトコルの四面体

2.1. トリレンマを超えて：第四の次元としての検証可能なコンプライアンス

ブロックチェーン設計における古典的な議論は、「分散化」「セキュリティ」「スケーラビリティ」という3つの目標を同時に最大化することはできないとする「ブロックチェーンのトリレンマ」を中心に展開されてきた。しかし、このフレームワークは、現代の金融インフラが直面

する重要な要件、すなわち規制遵守の必要性を見過ごしている。

再定義されたプロメテウス・プロトコルは、この設計空間に第四の重要な次元、すなわち「検証可能なコンプライアンス」を明示的に導入する。これにより、設計空間は三角形から四面体へと拡張される。これは単に規制に従うという受動的な姿勢を意味するものではない。コンプライアンスは、中央集権的で手動のオーバーレイではなく、プロトコルネイティブで、暗号学的に証明可能かつ自動化可能な機能となるシステムを創造することを意味する。

このアプローチは、分散化の目標と対立するものではない。むしろ、それを可能にするものである。従来の規制対応型システム（例：Ripple）は、許可された検証者セットを通じて中央集権化によってコンプライアンスを達成する。これに対し、プロメテウスは暗号技術（特にZKP）を用いて、コンプライアンスの「行為」を、準拠する主体の「アイデンティティ」から切り離す。参加者は、自身の身元を完全に明らかにすることなく、ルールを遵守していることを暗号学的に証明できる限り、パーミッションレスに参加できる。これにより、プロトコルは、検証者レベルでの高度な分散化と、規制コンプライアンスの両立という、従来は不可能とされた目標を達成できる。したがって、プライバシー＆監査可能性層（PAL）は単なるプライバシー層ではなく、分散化を可能にする層なのである。

2.2. 創発的な完全性の哲学：暗号経済システムによる信頼の強制

プロメテウスの第二の設計哲学は、「創発的な完全性」という概念に基づいている。これは、特定の参加者（例えば「評判の高い」発行者）の善意を信頼することを前提とするのではなく、すべての参加者が正直に行動することが最も収益性の高い戦略となるような、ゲーム理論的な構造を構築することを目指す。

このモデルでは、信頼はシステムの入力（assumption）ではなく、出力（emergent property）となる。プロトコルの完全性は、以下の2つのメカニズムの相互作用によって強制される。

1. **明示的な経済的インセンティブ:** ステーキング、報酬、そして悪意ある行動に対するスラッシング（罰金）を通じて、参加者の経済的合理性をプロトコルの安全性と一致させる。
2. **暗号学的に検証可能な証明:** 検証可能クレデンシャル（VC）とゼロ知識証明（ZKP）を用いて、参加者の属性や行動がプロトコルのルールに準拠していることを、信頼を必要とせずに検証可能にする。

この二重のメカニズムにより、システムは自己修正的かつ自己強化的になり、信頼は巧みに設計された暗号経済システムから自然に生まれる。

2.3. プロメテウスの設計空間における位置付け（図1）

この新しい設計目標を視覚化するため、四面体モデルを提案する。各頂点は「分散化」「セキュリティ」「スケーラビリティ」「検証可能なコンプライアンス」を表す。この立体内に、再設計されたプロメテウスが、他の主要なプロトコルと比較してプロットされる。

- **ビットコイン:** 高いセキュリティと分散化を達成するが、スケーラビリティと検証可能なコンプライアンスは低い。
- **イーサリアム:** よりバランスの取れたアプローチを取り、スケーラビリティの向上に注力

している。
- **Solana:** 高いスケーラビリティを達成するが、分散化の度合いは比較的低い。
- **プロメテウス:** 高いスケーラビリティ、強力なセキュリティ、そしてネイティブな検証可能コンプライアンスを独自に組み合わせることで、他のプロジェクトが最適化していないユニークな設計空間のニッチをターゲットとする。

この図は、プロメテウスが既存のプロトコルの単なる模倣ではなく、明確な目的意識を持って設計された、独自の価値提案を持つシステムであることを示している。

3. プロメテウス・アーキテクチャ：三層からなる共生システム

プロメテウスは、それぞれが特定の機能を担いながらも、相互に連携してプロトコル全体の目標を達成する、三層構造の共生的なアーキテクチャを採用している。

3.1. 第1層：アイデンティティ＆ガバナンス層（IGL） - 評判から検証可能な完全性へ

3.1.1. 純粋なプルーフ・オブ・レピュテーション（PoR）の批判とシビル攻撃の脆弱性

PoRは、エネルギー効率の良さや社会的信頼への依存といった理論的な強みを持つが、その主要な脆弱性はシビル攻撃にある。シビル攻撃とは、攻撃者が多数の偽のアイデンティティを安価に生成し、評判を不正に水増しすることで、ネットワークのコンセンサスを乗っ取る攻撃である。学術的分析と実世界のシステム障害が証明しているように、アイデンティティの生成に実質的な経済的コストがかからなければ、PoRは本質的に安全ではない。当初の設計で提案された、検証可能クレデンシャル（VC）への依存は、信頼の問題を曖昧に定義された「信頼できる」発行者へと単に転嫁するだけであり、それ自体が重大な中央集権化のベクトルを生み出す。

3.1.2. HPoSRソリューション：ハイブリッド・プルーフ・オブ・ステーク・アンド・レピュテーション

この根本的な脆弱性に対処するため、プロメテウスは経済的セキュリティと検証可能なアイデンティティを組み合わせたハイブリッドコンセンサスメカニズム、HPoSR（Hybrid Proof-of-Stake and Reputation）を導入する。

中核メカニズム:
検証者（Validator）となるためには、ノードは以下の2つの条件を同時に満たす必要がある。

1. **経済的ステーク（Economic Stake）:** PROトークンの最低限のステーク（例：100,000 PRO）をロックする。これにより、シビル攻撃を実行するための資本コストが法外に高くなり、プルーフ・オブ・ステーク（PoS）の実証済みセキュリティモデルがもたらされる。
2. **検証者クレデンシャル（Validator Credential）:** 後述するオンチェーントラスト・レジストリに登録された承認済み発行者から発行された、有効で失効していない特定のVCを保有する。これにより、各検証者アイデンティティが検証可能なオフチェーンのエンティティに紐付けられ、偽名のアイデンティティの大量生成が実質的に不可能になる。

乗数としての評判（Reputation as a Multiplier）:

HPoSRにおいて、評判はコンセンサスの重みを直接決定するものではない。代わりに、検証可能な履歴（稼働時間、検証の正確性、ガバナンスへの参加など）から導出される動的な評判スコアが、その検証者のステーキング報酬とコンセンサスプロセスにおける重みの「乗数」として機能する。これにより、高い評判が直接的に高い収益性につながるため、長期的な善意の行動に対する強力なインセンティブが生まれる。
評判スコア R は、エポック t ごとに以下の再帰式で更新される。

$$R_{i,t} = (1-\alpha) \cdot R_{i,t-1} + \alpha \cdot S_{i,t}$$

ここで、$R_{i,t-1}$ は検証者 i の前エポックにおける評判スコア、$S_{i,t}$ は現エポックの複合パフォーマンススコア、そして α は学習率（例：0.1）であり、過去の行動の重みを減衰させ、現在の行動を優先させる役割を果たす。複合スコア $S_{i,t}$ は、正規化された稼働時間（U）、検証の正確性（C）、ガバナンス参加（G）の加重平均として計算される。

$$S_{i,t} = w_U \cdot U_{i,t} + w_C \cdot C_{i,t} + w_G \cdot G_{i,t}$$

（重み付けの例：$w_U=0.4, w_C=0.4, w_G=0.2$）

このモデルは、評判を単なる参入障壁ではなく、継続的なパフォーマンスと直接連動した動的な経済資産へと昇華させる。

3.1.3. 発行者の統治：Trust over IP（ToIP）モデルに基づくオンチェーントラスト・レジストリ

VC発行者（銀行、政府機関、ID検証プロバイダーなど）への依存は、プロトコルに新たな中央集権化のリスクをもたらす可能性がある [1]。このエコシステムが適切に統治されなければ、プロトコルの分散化は名目的なものに過ぎなくなる。

このリスクを軽減するため、プロトコルは発行者エコシステムの統治哲学として、Linux FoundationがホストするTrust over IP（ToIP）の4層モデルを採用する [1]。ToIPは、インターネット規模のデジタルトラストを実現するための技術（機械層）とガバナンス（人間層）を組み合わせた包括的なアーキテクチャを提供する [1]。

- **第4層（アプリケーション層）：**特定のユースケース（例：国境を越えた送金アプリ）。
- **第3層（クレデンシャル交換層）：**VCがどのように要求され、提示されるかの標準化されたプロトコル（例：DIDComm）。
- **第2層（トラストスパニング層）：**すべてのエージェントを接続するプロメテウス・プロトコル自体。
- **第1層（トラストアンカー層）：**これが信頼の基点となる。プロメテウスは、承認されたすべてのVC発行者をリストアップする、分散型の**オンチェーントラスト・レジストリ**を実装する。

トラスト・レジストリで承認された発行者になるためには、事業体はPROトークンをステークし、プロメテウスDAOによるガバナンス承認プロセスを経る必要がある。これにより、信頼を確立するための許可制でありながら分散化されたシステムが構築される [4]。これらの発行者は、検証者（クレデンシャルに依存する事業体）から検証ごとに少額の手数料を請求するな

ど、持続可能なビジネスモデルを構築でき、競争力のある発行者市場の形成が促進される。

3.1.4. 表：HPoSRと他のコンセンサスアルゴリズムの比較

特徴	プルーフ・オブ・ワーク (PoW)	プルーフ・オブ・ステーク (PoS)	純粋なPoR	HPoSR (プロメテウス)
エネルギー消費	非常に高い	非常に低い	非常に低い	非常に低い
シビル攻撃耐性	非常に高い（計算コスト）	高い（資本コスト）	低い	非常に高い（資本コスト＋VC）
資本要件	高い（ハードウェア）	高い（ステーク）	なし	中程度（ステーク）
分散化の可能性	中程度（マイニングプールの集中化）	中程度（富の集中）	理論的には高いが、操作されやすい	高い（ステークと評判のバランス）
ペナルティメカニズム	なし（無駄なエネルギー）	スラッシング（資本没収）	評判の低下	スラッシング＋評判の低下

3.1.5. 図：IGLエコシステムの解説

以下の図は、IGLにおける参加者のライフサイクル全体を示している。このフローは、ユーザーが信頼できる現実世界のエンティティから始まり、プロトコルの検証者として活動し、その行動が継続的に評価されるという、検証可能な完全性のループを形成する。

1. **VC取得:** ユーザーは、オンチェーントラスト・レジストリに登録された承認済み発行者（例：銀行）からKYCベースのVCを取得する。
2. **DID作成と紐付け:** ユーザーはプロメテウス上で自身の分散型ID（DID）を作成し、取得したVCをそのDIDに紐付ける。
3. **検証者登録:** ユーザーはPROトークンをステークし、検証者クレデンシャルを提示して検証者ノードとなる。
4. **評判スコアの動的更新:** ノードはコンセンサスとガバナンスへの参加を開始し、その行動（稼働時間、投票の正確性など）に基づいて評判スコアがエポックごとに動的に更新される。

3.2. 第2層：トランザクション＆ファイナリティ層（TFL） - 決定論的な速度の達成

3.2.1. 曖昧なDAGファイナリティの批判

当初の設計が単純な有向非巡回グラフ（DAG）構造に依存していることは、絶対的で決定論的なファイナリティを必要とする金融取引には不十分である。初期のDAG実装（例：IOTAのTangle）における確率的ファイナリティの概念では、取引のセキュリティは時間とともに増加するものの、決して100%の確実性には達しない。これは高額な金融取引には受け入れられない。「チェックポイント」というアイデアは、IOTAがかつて採用していた中央集権的なコーディネーターに似た応急処置であり、単一障害点であるとして放棄されたモデルである。

3.2.2. ハイブリッドDAG-BFTアーキテクチャ：NarwhalとMysticetiの原則の統合

この重大な問題に対処するため、プロメテウスは、SuiやAptosのような高性能ブロックチェーンで実用性が証明されている最近の学術研究に触発された、最先端の2段階ファイナリティメカニズムを導入する[5]。このアーキテクチャは、トランザクションの

伝播と**順序付け**を分離することで、両方の世界の長所（DAGの高いスループットとBFTの決定論的ファイナリティ）を実現する。

フェーズ1：DAGベースのメモリプール（Narwhalに着想）
トランザクションは、まず構造化されたラウンドベースのDAGにブロードキャストされる 6。この層の主な目的は、トランザクションを効率的に伝播させ、その可用性を保証することである。

- **並列ブロック提案:** すべての検証者は並行してブロック（トランザクションのバッチ）を提案し、前のラウンドのブロック（具体的には2f+1個以上）を参照する[8]。これにより、取引の伝播と可用性の確保が、コンセンサスのクリティカルパスである順序付けから分離される。
- **可用性証明書（Certificate of Availability）:** 各ブロックは、他の検証者から2f+1個の署名を集めることで「可用性証明書」を獲得する[6]。これにより、そのブロックに含まれるデータが後続の順序付けフェーズで利用可能であることが保証される。この分離こそが、従来のBFTプロトコルが直面するリーダーのボトルネックを回避し、スループットを最大化する鍵となる[6]。

フェーズ2：BFTベースの順序付け（Mysticeti-Cに着想）
IGLから選出された高潔な検証者からなるローテーション委員会（後述のガバナンスにおける「公証人院」）がDAGを監視し、トランザクションの最終的な順序を決定する。

- **アンカーブロックの確定:** 各ラウンドで、委員会のリーダーがDAGから特定のブロック（「アンカー」）を次に順序付けられるものとして提案する[9]。
- **軽量BFTコンセンサス:** 委員会は、軽量なBFTコンセンサスプロトコル（Mysticeti-Cの変種を推奨）を実行してアンカーに合意する[10]。Mysticeti-Cは、明示的な証明書を必要とせず、DAG構造の解釈を通じて暗黙的に証明を行うことで、理論上の最小値である**3メッセージ遅延**でコミットを達成できるため、レイテンシを劇的に削減する[10]。
- **決定的ファイナリティ:** アンカーがBFTプロトコルによってコミットされると、DAG内でのその全因果履歴（そのアンカーに至るまでのすべての先行ブロック）が決定論的に確定し、順序付けられたと見なされる。これにより、金融台帳に不可欠な、絶対的で不可逆なファイナリティが提供される。

3.2.3. パフォーマンスと複雑性の分析

このハイブリッドモデルのパフォーマンス特性は、2つの層によって分離される。

- **スループット:** 主にDAG層のネットワーク帯域幅によって制限され、Narwhalベースのシステムが実証しているように、理論上50,000 TPS以上、場合によっては100,000 TPSを超える達成が可能である [6]。
- **ファイナリティまでのレイテンシ:** BFT層によって決定され、Mysticeti-Cのような最先端プロトコルを用いることで、WAN環境下でも**2秒未満**を目標とする [6]。SuiがBullsharkからMysticeti-Cに移行した際、レイテンシが4倍以上改善されたという実績は、この目標の達成可能性を強く示唆している [10]。

このアーキテクチャの実装は複雑であり、ビュー変更、ラウンド同期、因果的順序付けのための高度なロジックを伴うが、そのパフォーマンス上の利点は、この複雑性を正当化するものである。

3.2.4. 図：TFLトランザクションファイナリティフローの解説

以下の図は、TFLにおけるトランザクションの処理過程を示している。クライアントからのトランザクションがDAGを通じて伝播し、公証人院によって最終的に順序付けられ、確定するまでの流れを視覚化する。

!(https://i.imgur.com/tfl-flow.png "図3：TFLフロー")

1. **送信:** クライアントがトランザクション（Tx）を送信する。
2. **伝播とブロック化:** Txはネットワークにブロードキャストされ、DAGメモリプール内の複数の検証者ブロック（ラウンドR）に含まれる。
3. **アンカー提案:** ラウンドR+1の公証人院リーダーが、ラウンドRからアンカーブロックを提案する。
4. **BFT合意:** 評議会はMysticeti-CベースのBFTプロトコルを介してアンカーに投票する。
5. **コミットと確定:** アンカーがコミットされると、そのアンカーおよびその全因果履歴が確定（ファイナライズ）される。

3.3. 第3層：プライバシー＆監査可能性層（PAL） - 機密性とコンプライアンスの両立

3.3.1. ナイーブなZKP実装の批判とパフォーマンスのパラドックス

当初の設計のビジョンは強力だが、実用的には欠陥がある。ユーザーデバイスでのZKP生成のパフォーマンスコストを過小評価している。コンプライアンスに必要なような複雑な回路では、高性能CPU上であっても証明者時間が数百ミリ秒から数秒かかる可能性があり、これは「2秒のファイナリティ」というTFLの目標と矛盾する。また、「監査API」という概念も、暗号学的にどのように安全なアクセスが保証されるのか定義されておらず、セキュリティ上の懸念を残す。

3.3.2. 適応型ZKPと選択的開示による自動コンプライアンス

この層の中核は、プライバシーをデフォルトとしながら、検証可能なコンプライアンスと合法的な監査可能性を選択的に提供することにある。これを実現するために、プロトコルは複数の

戦略を組み合わせる。

クライアントサイドのパフォーマンス最適化:
ウォレットソフトウェアは、ZKPのUXを向上させるために複数の戦略を採用する。これには、頻繁に使用される回路の証明コンポーネントを事前計算すること、ネイティブに近いパフォーマンスを実現するためにWebAssembly（WASM）を活用すること、利用可能な場合は専用のハードウェアアクセラレータ（GPU、モバイルデバイスのNeural Processing Unitなど）を利用することが含まれる。
プロトコルレベルの適応型ZKP選択:
プロトコルは、タスクの要件に応じて異なるZKPスキームを適応的に使用する 12。

- **zk-SNARKs (例：Groth16, PLONK): ユーザーレベルの取引プライバシー**に主に使用される。その最大の利点は証明サイズが非常に小さい（数百バイト）ことであり、オンチェーンのストレージコストを最小限に抑える [13]。ただし、多くのSNARKsは信頼できるセットアップを必要とするというトレードオフがある [14]。
- **zk-STARKs: システムレベルの有効性証明**（例：将来的にプロメテウスがスケーラビリティのためにZKロールアップを実装する場合）に使用される。zk-STARKsの利点は、信頼できるセットアップが不要な「透明性」と、将来の量子コンピュータによる攻撃にも耐えうる「耐量子性」である [13]。その代償として、証明サイズはSNARKsよりも大きくなる。

自動コンプライアンスのための選択的開示:
これがPALの中核機能である。システムはZKPを使用して、基礎となるデータ（個人情報や取引額）を開示することなく規制遵守を証明する「コンプライアンス証明」を作成する。

- **FATFトラベルルール（勧告16）:** このルールは、特定の閾値を超える取引において、送金者と受取人の情報を共有することを義務付けている。ZKPを用いることで、送信者のウォレットは、「私はIGLトラスト・レジストリの信頼できる発行者からの有効なVCを所有しており、この証明はこの取引に暗号学的に拘束されている」という証明を生成できる。これにより、個人を特定できる情報（PII）自体をオンチェーンで明らかにすることなく、ルールが要求する当事者の適格性を証明できる。
- **AML閾値:** レンジプルーフ（範囲証明）というZKPの一種を使用して、「この取引の価値は報告義務のある閾値（例：10,000ドル）未満である」ことを、正確な金額を明らかにせずに証明できる。

3.3.3. 表：zk-SNARKsとzk-STARKsの比較

特徴	zk-SNARKs	zk-STARKs
信頼できるセットアップ	ほとんどの方式で必要 [13]	不要（透明性） [13]
証明サイズ	小さい（数百バイト） [13]	大きい [13]
検証時間	速い [12]	SNARKsより遅い [12]

耐量子性	脆弱（楕円曲線暗号に依存） [14]	安全（ハッシュ関数に依存） [13]
主なユースケース	プライバシー（例：Zcash）、スケーリング（例：zkSync） [12]	スケーリング（例：StarkNet）、透明性が重要なシステム [12]

3.3.4. 監査可能な「ビューキー」：閾値暗号による令状付きバックドア

システム全体のプライバシーを損なうことなく、合法的な情報要求（例：裁判所の令状）にどのように対応するか。単一のエンティティがアクセスできるマスターキーは、分散化の原則に反する。

この課題に対する解決策として、プロメテウスは**閾値暗号**に基づく分散型アクセス制御メカニズムを実装する [17]。

- **データ暗号化:** 各トランザクションの機密データは、一意の対称鍵で暗号化される。
- **鍵の分割:** この対称鍵を復号するための鍵は、Shamirの秘密分散法のような閾値秘密分散法を用いて、複数のシェア（断片）に分割される [19]。
- **シェアの配布:** これらのシェアは、「認可ノード」（公証人院がこの役割を兼任）の分散型セットに配布される。
- **分散型復号プロセス:** 鍵を再構築して取引データを復号するには、これらの認可ノードの閾値数（例：n個中t個、通常はt≥32·n）が、それぞれのシェアを提供して協力する必要がある [21]。
- **ガバナンスによるトリガー:** この協力プロセスは、正当なオフチェーンの法的命令（令状など）を根拠とする、有効なオンチェーンガバナンス提案が可決された場合にのみトリガーできる。

このメカニズムにより、プロジェクト開発者を含むいかなる単一の当事者による一方的なデータアクセスも防がれ、例外的アクセスのための堅牢で監査可能かつ分散化されたプロセスが構築される [21]。

3.3.5. 図：コンプライアンス準拠のトランザクションライフサイクル解説

以下のシーケンス図は、PALを通じてコンプライアンスを遵守した取引がどのように行われるかを示している。このプロセスは、ユーザーのプライバシーを最大限に保護しつつ、規制要件を自動的に満たすように設計されている。

1. **取引構築:** アリスのウォレットがボブへの取引を構築する。
2. **ルール取得:** ウォレットは、適用されるコンプライアンスルールセットをプロトコルから取得する。
3. **ZKP生成:** ウォレットは、取引がこれらのルールに準拠していることを証明するZKPをクライアントサイドで生成する。
4. **送信:** 取引ペイロードは、生成されたZKPと共にTFLに送信される。

5. **検証:** TFLの検証者は、取引の機密データを見ることなく、ZKPを迅速に検証する。証明が有効であれば、取引はファイナリティプロセスに進む。

4. PROトークン：多角的な経済モデル

PROトークンは、単なる投機的資産としてではなく、ネットワークのセキュリティ、運用、およびガバナンスに不可欠な中核的なユーティリティ手段として設計されている。

4.1. トークノミクス・フレームワークと中核的ユーティリティ

- **供給と配分:** 希少性を確保し、長期的な価値の保存を促進するため、総供給量を100億トークンに固定する。初期配分は、創設チーム/投資家（4年間の権利確定期間付きで20%）、エコシステム開発基金（50%）、そしてコミュニティへのエアドロップおよび初期流動性インセンティブ（30%）に、事前に定義された割合で割り当てられる。
- **中核的ユーティリティ:**
  - **ステーキング:** PROは、HPoSRコンセンサスメカニズム（第1層）における検証者としての参加、および承認されたVC発行者になるために必要な必須資産である。
  - **ガバナンス:** PROは、後述する二院制ガバナンスシステムのトークン院における議決権を付与する。
  - **手数料メカニズム:** これが経済モデルの核心である。

4.2. 価値の蓄積とデフレ圧力：手数料焼却メカニズム

ユーザーコストの予測可能性を高めるため、取引手数料はステーブルコイン（例：USDC）で支払われる。これは、ネイティブトークンの価格変動からユーザーを保護し、UXを向上させるための重要な設計である。しかし、これだけではPROトークンの価値とネットワークの経済活動が結びつかない。

この問題を解決するため、プロトコルはイーサリアムのEIP-1559に触発された、洗練された手数料メカニズムを導入する [22]。

1. **手数料の徴収:** ネットワークで発生した取引手数料（USDC）は、プロトコルの財務省に集められる。
2. **買い戻しと焼却（Buyback and Burn）:** この手数料収入の一定割合（例：初期設定10%、ガバナンスにより変更可能）が、プロトコルによってプログラム的に、分散型取引所などの公開市場からPROトークンを買い戻すために使用される。
3. **供給削減:** 買い戻されたPROトークンは、永久に流通から取り除くために焼却（バーン）される。

このメカニズムは、ネットワークの経済活動（取引量）とPROトークンの価値との間に直接的な正のフィードバックループを生み出す。プラットフォームが成長し、より多くの取引が処理されるにつれて、より多くの手数料が生成され、より多くのPROが市場から買い戻されて焼却される。この継続的な買い圧力と供給削減により、PROはデフレ資産となり、長期保有者とステーカーに報酬を与える [22]。これは、ネットワークの成功が直接トークン保有者に還元される、強力な価値蓄積モデルである。

4.3. セキュリティの経済学：ステーキング報酬とスラッシング条件

- **ステーキング報酬:** 検証者が受け取る報酬は、複数の要因によって動的に決定される。これには、ネットワーク全体の参加率に応じて調整される基本発行率（年率2-5%）、ノードの評判スコア（Ri,t）による乗数、およびそのエポックで処理された取引手数料の分配が含まれる。この複合的な報酬体系は、単なる資本の提供だけでなく、高性能で誠実な運用を継続的に行うことへのインセンティブを与える。
- **スラッシング・ペナルティ:** 悪意のある行動（例：TFLのBFT層での二重署名、不正な取引の検証）は、検証者のステークされたPROの大部分（最大50%）がスラッシング（没収）されるという厳しい結果を招く。この経済的ペナルティの規模は、攻撃から得られる潜在的な利益よりも常に大きくなるように設計されなければならない。これにより、ゲーム理論的な観点から、誠実な参加が唯一の合理的な戦略であることが保証される。

5. 長期的な安定性のための二院制ガバナンス・フレームワーク

5.1. DAOガバナンスの問題点：衆愚政治と寡頭制

標準的なトークン加重投票（1トークン＝1票）は、「クジラ」として知られる大口トークン保有者によるガバナンスの乗っ取り（衆愚政治、Plutocracy）に対して脆弱である [26]。一方で、純粋な評判ベースのシステムは、初期の参加者が不当な影響力を持ち続ける寡頭制（Oligarchy）につながる可能性がある。これらの問題は、既存のDAOガバナンスにおいて十分に文書化されている [27]。

5.2. 提案される解決策：二院制システム

これらの根深い課題に対処するため、プロメテウスは米国の議会のような現実世界の統治構造や、LidoやOptimismといった先進的なDAOの実験から着想を得た**二院制（Bicameral）ガバナンスシステム**を採用する [29]。このシステムは、異なるステークホルダーグループの利益を代表する2つの議院で構成され、権力の抑制と均衡を図る。

- **トークン院 (Token House):**
  - **構成:** 全てのPROトークン保有者。
  - **議決権:** 保有量に比例する（1トークン＝1票）。
  - **責務:** プロトコルの**資本的・経済的利益**を代表する。財務省からの助成金、手数料焼却率の調整、エコシステムプロジェクトへの資金提供など、経済的パラメータに関連する提案について投票する責任を負う。
- **公証人院 (Notary House):**
  - **構成:** IGLのトップランクの検証者ノード（TFLの公証人評議会のメンバーと同一）。
  - **議決権:** 評判に基づいて重み付けされる（1高評判検証者＝1票）。
  - **責務:** プロトコルの**運用的・技術的利益**を代表する。技術的なプロトコルアップグレード、コンセンサスルールの変更、セキュリティパラメータの調整など、ネットワークの健全性と安定性に直接影響を与える提案に責任を負う。

この構造は、異なる種類のステークホルダー（資本提供者とインフラ運用者）に、それぞれの専門分野に応じた権限を与えることで、より専門的で質の高い意思決定を促進する [29]。

5.3. 表：二院制ガバナンスの責任範囲

議院	構成員	議決権メカニズム	権限の範囲（主な責務）
トークン院	全PROトークン保有者	1トークン = 1票	**経済的・財務的決定** - 手数料パラメータ（焼却率など）の調整 - エコシステム基金からの助成金承認 - 財務省の資産運用方針
公証人院	高評判の検証者ノード	1高評判検証者 = 1票	**技術的・セキュリティ的決定** - プロトコルのコアアップグレード - コンセンサス・ルールの変更 - セキュリティパラメータ（スラッシング率など）の調整

5.4. 抑制と均衡、および紛争解決

このシステムの真価は、二院間の抑制と均衡（Checks and Balances）のメカニズムにある[29]。

- **憲法的原則:** プロトコルは、プライバシーへのコミットメントや三層アーキテクチャなど、変更が非常に困難な一連の中核原則（「プロトコル憲法」）に基づいて設立される。これらの原則の変更には、両院での超多数決（例：75%以上）が必要となる。
- **提案プロセス:** ほとんどの主要な提案（例：重要なプロトコルアップグレード）は、両院での単純多数決による可決が必要となる。これにより、変更が経済的に健全（トークン院の承認）かつ技術的に堅牢（公証人院の承認）であることが保証される。この構造は、一方の議院が他方の議院に一方的に意思を押し付けることを防ぐ。
- **紛争解決:** 立法上の膠着状態（デッドロック）に陥った場合の、段階的なエスカレーションを含む正式な紛争解決メカニズムが定義される。

このモデルは、Lidoのデュアルガバナンスのような最近のDAOの革新からも着想を得ており、異なるステークホルダーグループ間の力のバランスをとることで、長期的なプロトコルの安定性と予測可能性を高めることを目指している[27]。

6. ユーザーエクスペリエンス（UX）と採用戦略

6.1. 複雑性の抽象化

プロトコルの成功は、その強力な機能をエンドユーザーにとってシームレスで直感的な体験に変換できるかどうかにかかっている。平均的なユーザーは、DID、VC、ZKPの技術的詳細を理解する必要はない。ウォレットソフトウェアは、この複雑性を完全に抽象化しなければならない。例えば、VCを取得するプロセスは、従来のアプリでIDを検証するのと同様に、ウォレットのオンボーディングフローに直接統合され、ガイド付きでなければならない。

6.2. シードフレーズを超えて：安全で使いやすい鍵管理

従来の12単語または24単語のシードフレーズは、ユーザーが自己管理する上で単一障害点であり、紛失や盗難のリスクが高く、主流の採用における主要なUXの障壁となっている。プロメテウスエコシステムは、この問題を解決するため、2つの先進的な鍵管理ソリューションをネイティブにサポートする。

1. ソーシャルリカバリー（Social Recovery）
Argentウォレットなどの先駆的な実装に触発されたこのメカニズムは、ユーザーフレンドリーな回復経路を提供する 31。

- **仕組み:** ユーザーは、信頼できる「ガーディアン」（友人、家族、または自身の他のハードウェアウォレットなど）のセットを指定する。鍵を紛失した場合、これらのガーディアンの閾値数（例：5人中3人）が集合的に回復要求を承認することで、ユーザーは新しいデバイスでウォレットへのアクセスを回復できる [20]。
- **利点:** 信頼を分散させ、シードフレーズの単一障害点を排除する。日常のトランザクションは単一の署名キーで迅速に行えるため、利便性を損なわない [31]。

2. マルチパーティ計算（Multi-Party Computation, MPC）
機関投資家や最高のセキュリティを求めるユーザー向けに、MPCは鍵管理のパラダイムを根本から変える 35。

- **仕組み:** 単一の秘密鍵がそもそも存在しない。代わりに、鍵は複数の「シェア」に暗号学的に分割され、異なる当事者（例：ユーザーのモバイルデバイス、ラップトップ、セキュアなサーバー）によって独立して保持される [38]。トランザクションに署名するには、これらのシェアが協力して分散型の暗号計算を実行し、完全な鍵を再構築することなく有効な署名を生成する [36]。
- **利点:** 単一のデバイスやサーバーが侵害されても資金が盗まれることはないため、単一障害点を完全に排除する。FireblocksやZenGoといった企業によって、その有効性は実証済みである [35]。

6.3. 市場投入戦略：創設コンソーシアムと段階的展開

信頼できるVC発行者に依存するネットワークには、ブートストラップの問題、すなわち「鶏が先か卵が先か」という問題がある。発行者はユーザーなしでは参加するインセンティブがなく、ユーザーは有用なクレデンシャルを発行してくれる発行者がいなければ参加しない。

創設コンソーシアム（Founding Consortium）：
この問題を解決するため、プロジェクトは、ID検証会社、金融機関、そして潜在的には政府機関を含む初期パートナーの「創設コンソーシアム」と共に立ち上げられる。これらのパート

ナーは、最初の承認された発行者として機能し、ユーザーと検証者を引き付けるために必要な初期の高価値クレデンシャル（例：KYC/AML証明、認定投資家証明）を提供する。この戦略的提携により、ネットワークは初日から実用的なユーティリティを持つことが保証される。
段階的な展開とターゲットユースケース:
プロトコルは、一度にすべての問題を解決しようとはしない。初期の焦点は、プロメテウスが既存のソリューションに対して明確な10倍の改善を提供する、特定の、痛みの大きいユースケースに置かれる。

- **フェーズ1：国境を越えた送金とB2B決済:** これらの市場は、現在、高額な手数料、遅い決済時間（数日）、そして複雑なコンプライアンスの摩擦に悩まされている。プロメテウスの低手数料、ほぼ即時の決定的ファイナリティ、そしてPALによって自動化された組み込みのコンプライアンスは、説得力のある代替案を提供する。
- **フェーズ2：コンプライアンス準拠の分散型金融（DeFi）:** PALを活用して、DeFiプロトコルが既存の規制の枠組み内で運営できるようにする。これにより、コンプライアンス上の懸念からこれまで参加をためらっていた機関投資家の資本（数兆ドル規模）が、分散型金融の世界に流入する道が開かれる。
- **フェーズ3：マイクロペイメントとIoT:** プロトコルの極めて低い取引コストと高いスループットを活用して、コンテンツクリエイターへのリアルタイムの支払い、機械間の自動決済など、これまで経済的に成り立たなかった新たな経済モデルを実現する。

7. 結論：分散型金融の新たな道を切り拓く

本報告書で詳述されたアーキテクチャの改善ー純粋なPoRから経済的インセンティブを持つHPoSRへの移行、確率的ファイナリティから決定的ファイナリティを保証するハイブリッドDAG-BFTモデルの導入、そして閾値暗号を用いた監査可能なプライバシー層の実装ーは、当初のビジョンが直面していた根本的な技術的および哲学的課題に対処するものである。

再定義されたプロメテウスが選択する中核的なトレードオフは明確である。それは、ビットコインの参入点における絶対的でパーミッションレスな匿名性を、検証可能な偽名アイデンティティのシステムのために犠牲にすることである。その見返りとして、プロメテウスは、規制され、プライバシーを保護する新しいグローバル金融システムの基盤層として機能するために必要な速度、スケーラビリティ、および規制上の互換性を獲得する。

これは妥協ではなく、主流の採用を達成するための意図的かつ必要な設計上の選択である。このプロトコルは、分散型技術の理想と現実世界の金融システムの要件との間の橋渡しとなることを目指しており、それによって金融の未来における独自の、そして不可欠な位置を確立する。

付録A：用語集

- **BFT (Byzantine Fault Tolerance):** ビザンチン故障耐性。システム内の一部のコンポーネントが故障したり、悪意を持って動作したりしても、システム全体が正常に機能し続ける能力。
- **DAG (Directed Acyclic Graph):** 有向非巡回グラフ。ブロックが直線的なチェーンではな

く、グラフ構造で相互にリンクされるデータ構造。並列処理を可能にし、スループットを向上させる。
- **DID (Decentralized Identifier):** 分散型ID。中央集権的な登録機関に依存せず、個人や組織が自身でコントロールできるグローバルに一意な識別子。
- **HPoSR (Hybrid Proof-of-Stake and Reputation):** ハイブリッド・プルーフ・オブ・ステーク・アンド・レピュテーション。経済的なステークと検証可能な評判スコアを組み合わせた、プロメテウス独自のコンセンサスアルゴリズム。
- **MPC (Multi-Party Computation):** マルチパーティ計算。複数の当事者が、それぞれの秘密情報を明かすことなく、共同で計算を実行するための暗号技術。鍵管理において単一障害点を排除するために使用される。
- **シビル攻撃 (Sybil Attack):** 攻撃者が多数の偽のアイデンティティを作成し、ネットワーク内で不当に大きな影響力を行使しようとする攻撃。
- **スラッシング (Slashing):** 検証者が悪意のある行動（例：二重署名）を行った場合に、そのステークされた資産の一部または全部を没収する罰則メカニズム。
- **閾値暗号 (Threshold Cryptography):** 暗号鍵を複数のシェア（断片）に分割し、操作（署名や復号）を実行するために一定数（閾値）以上のシェアの協力が必要となる暗号技術。
- **ToIP (Trust over IP):** Linux Foundationがホストする、インターネット規模のデジタルトラストを実現するための標準とアーキテクチャを開発するプロジェクト。
- **VC (Verifiable Credential):** 検証可能クレデンシャル。発行者によって暗号学的に署名された、特定の属性（例：「18歳以上である」）に関するデジタルな証明書。
- **ZKP (Zero-Knowledge Proof):** ゼロ知識証明。ある陳述が真実であることを、その陳述以外のいかなる情報も明かすことなく証明するための暗号学的手法。
- **zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):** ZKPの一種。証明サイズが非常に小さく（Succinct）、検証者と証明者の間の対話が不要（Non-Interactive）であることが特徴。
- **zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge):** ZKPの一種。信頼できるセットアップが不要（Transparent）で、計算量の大きな問題に対してもスケーラブルであることが特徴。耐量子性も持つ。

付録B：参考文献

- [1] Trust Over IP - LF Decentralized Trust.
- [4] Dhiway. Trust over IP: A complete architecture for internet-scale digital trust.
- [2] Trust over IP (ToIP) Technology Architecture Specification - GitHub Pages.
- [3] Trust Over IP Foundation - YouTube.
- [40] Decentralized-ID.com. Trust over IP.
- [6] Danezis, G., et al. (2022). Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus.
  EuroSys '22.
- [8] Danezis, G., et al. (2021). Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus.
  arXiv:2105.11827.

- [7] Salem, A. (2021). A review of Narwhal and Tusk: A DAG-based mempool and efficient BFT consensus.
  Medium.
- [11] Danezis, G., et al. (2024). Mysticeti: Reaching the Latency Limits with Uncertified DAGs.
  NDSS Symposium.
- [10] Danezis, G., et al. (2024). MYSTICETI: Reaching the Latency Limits with Uncertified DAGs.
  arXiv:2310.14821.
- [5] BlockScholes. (2024). Mysticeti – The Consensus Mechanism of Sui.
- [9] Gupta, A. (2024). All you need is DAG #4- Mysticeti.
  Medium.
- [14] Panther Protocol. (2023). zk-SNARKs vs zk-STARKs — Comparing Zero-knowledge Proofs.
- [12] QuillAudits. (2024). zk-STARK vs zk-SNARK : An In-Depth Comparative Analysis.
- [13] Cyfrin. (2024). A Full Comparison: What are zk-SNARKs and zk-STARKS?
- [16] Horizen. (2023). zk-SNARKs vs zk-STARKs.
- [15] Calibraint. (2024). ZK-SNARK vs STARK: Differences & Comparison.
- [41] Cevallos, A., et al. (2025). Thetacrypt: A Distributed Service for Threshold Cryptography.
  arXiv:2502.03247.
- [17] Cevallos, A., et al. (2025). Thetacrypt: A Distributed Service for Threshold Cryptography.
  arXiv:2502.03247.
- [18] NIST. (2023). Threshold Cryptography Project.
- [19] Wikipedia. Threshold cryptosystem.
- [21] Watson, E. (2025). Threshold cryptography and the future of wallet UX.
  Bobsguide.
- [29] Gate.com. (2023). Ambition made to counteract ambition - DAO governance and bicameralism.
- [30] Optimism Collective. Welcome to the Collective.
- [26] Frontiers in Blockchain. (2025). The Dual Imperative: Forging Resilient Governance in Decentralized Autonomous Organizations.
- [27] ResearchGate. (2025). Exploring Decentralized Autonomous Organization (DAO) Governance: An integrative literature review.
- [28] Goldin, D., et al. (2023). A Survey of Research on Decentralized Autonomous Organizations (DAOs).
  arXiv:2310.19201.
- [22] Galaxy Digital. (2021). EIP-1559: The Final Puzzle Piece to Ethereum's Monetary Policy.
- [23] Collective Shift. (2021). All About EIP-1559.
- [25] The Defiant. (2021). EIP-1559 Explained: The Fee Burning Upgrade That Has ETH Miners in a Fit.
- [24] Monnot, B., et al. (2021). Dynamical Analysis of the EIP-1559 Ethereum Fee Market.
  ACM Conference on Advances in Financial Technologies.

- [31] Cyfrin Updraft. Social Recovery Wallets.
- [34] Reddit. (2023). Are you using social recovery for your crypto wallets?
- [32] Gate.com. (2023). What is a Social Recovery Wallet?
- [33] Decrypt. (2020). Argent wallet review: DeFi made easy.
- [20] Gnanasekar, A., et al. (2023). Smart Contract-Based Social Recovery Wallet Management Scheme for Digital Assets.
  ResearchGate.
- [35] Fireblocks. Wallets-as-a-Service.
- [38] Fireblocks. (2023). Digital Asset Custody and Transaction Processing: Leading Practices Using Fireblocks MPC Solution.
- [36] Fireblocks. What is MPC (Multi-Party Computation)?
- [37] ZenGo. What is an MPC Wallet?
- [39] ZenGo. Zengo Business: The Crypto Wallet for Business.
- [10] Danezis, G., et al. (2024). MYSTICETI: Reaching the Latency Limits with Uncertified DAGs.
  arXiv:2310.14821.
- [6] Danezis, G., et al. (2021). Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus.
  arXiv:2105.11827.
- [10] Danezis, G., et al. (2024). MYSTICETI: Reaching the Latency Limits with Uncertified DAGs.
  arXiv:2310.14821.

引用文献

1. Trust Over IP - LF Decentralized Trust, 8月 8, 2025にアクセス、https://www.lfdecentralizedtrust.org/projects/trust-over-ip
2. ToIP Technical Architecture Specification - GitHub Pages, 8月 8, 2025にアクセス、https://trustoverip.github.io/TechArch/
3. Trust Over IP Foundation - YouTube, 8月 8, 2025にアクセス、https://www.youtube.com/channel/UC7gD2mHX_AXzkTHelj2nYEA
4. Trust Over IP — A complete architecture for Internet-scale digital trust - Dhiway, 8月 8, 2025にアクセス、https://dhiway.com/trust-over-ip-a-complete-architecture-for-internet-scale-digital-trust/
5. Mysticeti – The Consensus Mechanism of Sui - Block Scholes, 8月 8, 2025にアクセス、https://www.blockscholes.com/premium-research/mysticeti-the-consensus-mechanism-of-sui
6. Narwhal and Tusk: A DAG-based Mempool and Efficient BFT ... - arXiv, 8月 8, 2025にアクセス、 https://arxiv.org/pdf/2105.11827
7. A review of Narwhal and Tusk: A DAG-based mempool and efficient BFT consensus., 8月 8, 2025にアクセス、https://salemal.medium.com/a-review-of-narwhal-and-tusk-a-dag-based-mempool-and-efficient-bft-consensus-bf2099908c63
8. Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus - ar5iv, 8月 8,

2025にアクセス、 https://ar5iv.labs.arxiv.org/html/2105.11827
9. All you need is DAG #4-Mysticeti - Medium, 8月 8, 2025にアクセス、 https://medium.com/@amangupta432005/all-you-need-is-dag-4-mysticeti-6ea73e0d38d6
10. MYSTICETI: Reaching the Latency Limits with Uncertified DAGs - arXiv, 8月 8, 2025にアクセス、 https://arxiv.org/pdf/2310.14821
11. Mysticeti: Reaching the Latency Limits with Uncertified DAGs - NDSS Symposium, 8月 8, 2025にアクセス、 https://www.ndss-symposium.org/ndss-paper/mysticeti-reaching-the-latency-limits-with-uncertified-dags/
12. zk-STARK vs zk-SNARK : An In-Depth Comparative Analysis - QuillAudits, 8月 8, 2025にアクセス、 https://www.quillaudits.com/blog/ethereum/zk-starks-vs-zk-snarks
13. Full Guide to Understanding zk-SNARKs and zk-STARKS - Cyfrin, 8月 8, 2025にアクセス、 https://www.cyfrin.io/blog/a-full-comparison-what-are-zk-snarks-and-zk-starks
14. zk-SNARKs vs zk-STARKs — Comparing Zero-knowledge Proofs - Panther Protocol, 8月 8, 2025にアクセス、 https://blog.pantherprotocol.io/zk-snarks-vs-zk-starks-differences-in-zero-knowledge-technologies/
15. Decoding ZK-SNARK VS STARK: An In-Depth Comparative Analysis - Calibraint, 8月 8, 2025にアクセス、 https://www.calibraint.com/blog/zk-snark-vs-stark-differences-comparison
16. zk-SNARKs vs zk-STARKs | Horizen Academy, 8月 8, 2025にアクセス、 https://www.horizen.io/academy/zk-snarks-vs-zk-starks/
17. Thetacrypt: A Distributed Service for Threshold Cryptography - arXiv, 8月 8, 2025にアクセス、 https://arxiv.org/html/2502.03247v1
18. Multi-Party Threshold Cryptography | CSRC - NIST Computer Security Resource Center, 8月 8, 2025にアクセス、 https://csrc.nist.gov/projects/threshold-cryptography
19. Threshold cryptosystem - Wikipedia, 8月 8, 2025にアクセス、 https://en.wikipedia.org/wiki/Threshold_cryptosystem
20. Smart Contract-Based Social Recovery Wallet Management Scheme for Digital Assets, 8月 8, 2025にアクセス、 https://www.researchgate.net/publication/371515274_Smart_Contract-Based_Social_Recovery_Wallet_Management_Scheme_for_Digital_Assets
21. Security without sacrifice: Threshold cryptography and the future of wallet UX | bobsguide, 8月 8, 2025にアクセス、 https://www.bobsguide.com/threshold-cryptography-and-the-future-of-wallet-ux/
22. EIP-1559: A Major Upgrade for Ethereum - Galaxy, 8月 8, 2025にアクセス、 https://www.galaxy.com/insights/research/eip-1559-major-ethereum-upgrade
23. All About EIP-1559 - Ethereum - Collective Shift, 8月 8, 2025にアクセス、 https://collectiveshift.io/ethereum/eip-1559-guide/
24. Dynamical Analysis of the EIP-1559 Ethereum Fee Market - the King's College London Research Portal, 8月 8, 2025にアクセス、 https://kclpure.kcl.ac.uk/portal/files/180741130/EIP1559.pdf
25. Here's How EIP-1559 Changes the Economics of Ethereum - "The Defiant", 8月 8, 2025にアクセス、 https://thedefiant.io/news/research-and-opinion/eip-1559-economics
26. Decentralizing governance: exploring the dynamics and challenges of digital commons and DAOs - Frontiers, 8月 8, 2025にアクセス、 https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1538227/full

27. (PDF) Exploring Decentralized Autonomous Organization (DAO) Governance: An integrative literature review - ResearchGate, 8月 8, 2025にアクセス、https://www.researchgate.net/publication/385694204_Exploring_Decentralized_Autonomous_Organization_DAO_Governance_An_integrative_literature_review
28. Open Problems in DAOs - arXiv, 8月 8, 2025にアクセス、https://arxiv.org/html/2310.19201v2
29. Ambition made to counteract ambition - DAO governance and bicameralism - Gate.com, 8月 8, 2025にアクセス、https://www.gate.com/learn/articles/ambition-made-to-counteract-ambition-dao-governance-and-bicameralism/1218
30. Welcome to the Optimism Collective, 8月 8, 2025にアクセス、https://community.optimism.io/welcome/welcome-overview
31. Social Recovery Wallets - Web3 Wallet Security Basics, 8月 8, 2025にアクセス、https://updraft.cyfrin.io/courses/web3-wallet-security-basics/signer-basics/social-recovery-wallets
32. What is a Social Recovery Wallet? - Gate.com, 8月 8, 2025にアクセス、https://www.gate.com/learn/articles/what-is-a-social-recovery-wallet/676
33. Argent wallet review: DeFi made easy - Decrypt, 8月 8, 2025にアクセス、https://decrypt.co/30330/argent-wallet-review-defi-made-easy
34. Are you using social recovery for your crypto wallets? : r/CryptoCurrency - Reddit, 8月 8, 2025にアクセス、https://www.reddit.com/r/CryptoCurrency/comments/14fz3l9/are_you_using_social_recovery_for_your_crypto/
35. Wallets-as-a-Service | Fireblocks, 8月 8, 2025にアクセス、https://www.fireblocks.com/platforms/wallets-as-a-service/
36. What Is MPC (Multi-Party Computation)? - Fireblocks, 8月 8, 2025にアクセス、https://www.fireblocks.com/what-is-mpc/
37. MPC Wallet - What is MPC? - Zengo, 8月 8, 2025にアクセス、https://zengo.com/mpc-wallet/
38. Digital Asset Custody and Transaction Processing Leading Practices Using Fireblocks' MPC solution, 8月 8, 2025にアクセス、https://www.fireblocks.com/report/digital-asset-custody-and-transaction-processing-leading-practices-using-fireblocks-mpc-solution/
39. Crypto Wallet for Business - Zengo, 8月 8, 2025にアクセス、https://zengo.com/business/crypto-wallet-for-business/
40. Trust over IP Foundation - TOIP | Verifiable Credentials and Self Sovereign Identity Web Directory, 8月 8, 2025にアクセス、https://decentralized-id.com/organizations/trustoverip/
41. arxiv.org, 8月 8, 2025にアクセス、https://arxiv.org/html/2502.03247v1#:~:text=Practical%20applications,-Report%20issue%20for&text=Many%20current%20projects%20integrate%20threshold%20schemes%20with%20blockchains.&text=For%20example%2C%20threshold%20cryptography%20can,and%20are%20executed%20%5B14%5D%20.